providing either virtual collocation and/or escorts for CRTEE arrangements; and (5) converting existing physical collocation arrangements to virtual collocation in selected, highly sensitive security risk COs. These proposed security measures are appropriate, reasonable, in the public interest, and necessary to ensure the security, reliability and safety of Verizon MA's telecommunications infrastructure in today's environment based on the Company's network architecture.

Q. Please briefly describe Verizon MA's network architecture.

A. Verizon MA provides the backbone platform for data, voice, and long distance services for its end-user and carrier customers. Generally Verizon MA's network consists of three basic components: (1) network access or loop facilities; (2) central office buildings that contain switching, transmission, power plant and other support system equipment; and (3) interoffice transmission facilities. A diagram of this basic network design and a more detailed description of the various network components are appended to this testimony as Attachment 3.

As described in Attachment 3, the CO is the "hub" where network access lines and interoffice facilities are combined to connect with other facilities to provide telecommunications services to residence and business customers, including governmental, financial and public safety organizations, as well as to carrier customers that interconnect their networks to Verizon or subscribe to its wholesale or retail services. All of those customers depend on the reliability of Verizon MA's telecommunications network. Moreover, based on current

technology and network configurations, any inadvertent or intentional damage in a given CO may impair multiple end offices with potentially significant service-affecting consequences, including but not limited to the interruption of public safety or emergency services.

At the time that COs were originally built, they were designed to make efficient use of space and ensure that all of the equipment interconnected and functioned properly.[20] Likewise, the COs evolved over time, with equipment being placed where it made the most technical sense. COs were not, however, designed to accommodate or house equipment used by multiple carriers. For that reason, the CO building structure itself (*i.e.*, the exterior walls and doors of the premises) was the primary security measure to keep unauthorized individuals out.

Since the establishment of COs, circumstances have changed with the introduction of physical collocation. Physical collocation– and, in particular, cageless collocation or CCOE – inherently compromise Verizon MA's ability to protect its network *within* the CO.[21]

---

[20] For example, equipment with similar functions is grouped together; room for growth is planned for equipment, such as switches and frames, that must be contiguous; certain equipment (*e.g.*, power plant, circuit switches, interoffice and toll transmission equipment) may be segregated for technical and safety reasons; and infrastructure (*e.g.*, power, heating, ventilation, air conditioning, etc.) is designed to support each component. In addition, switches and transmission equipment are on different ground planes (*i.e.*, isolated versus integrated) and cannot be commingled for safety and personnel reasons.

[21] If new COs were built today, Verizon MA could design them with *interior* security in mind, and for example, place all of its sensitive equipment on one floor, and leave other parts of the CO with empty space for collocators. Verizon MA could also ensure that all the empty space in the CO was near a door that could be adequately secured.

Q. Please describe the effect of Verizon MA's network architecture on the types of security measures proposed.

A. Because of the critical and highly sensitive nature of the equipment located in Verizon MA's COs and the far-reaching effects of a network outage,[22] access to COs with physical collocation arrangements creates significant risks for Verizon MA and the end-user and carrier customers served by those COs. This is particularly true in COs with tandem switches, Signal Transfer Points ("STPs"), or emergency 911 ("E911") switches and adjunct equipment, each of which is critical to the network as they are used to complete interoffice and emergency calls. Although existing security measures, such as security cameras and badges with computerized tracking systems, may afford some protection, they alone cannot prevent damage to Verizon MA's network infrastructure.

Because of the design of COs, placing locked cabinets around Verizon MA's equipment and network is neither a technically feasible nor an economically viable option. Accordingly, to address these legitimate security concerns, Verizon MA should be permitted to apply a general policy of *secure* segregation and separation of its equipment areas and collocator equipment areas, and should be allowed to migrate physical collocation arrangements that do not comply with that standard. Contrary to the FCC conditions currently on appeal, Verizon MA

[22] Not only is inadvertent or intentional damage to the CO's operational and electronic equipment a concern, but also damage to its power plant and environmental support infrastructure (*e.g.*, water supply, heating, ventilation, and air conditioning system, etc) must be prevented.

should not be limited to requiring separate space only where no additional time or costs would be incurred. 47 C.F.R. §51.323(i)(4). The security risks to the network far outweigh these restrictions.

Currently, traditional "caged" physical collocation and SCOPE are provided in separate, secured areas of Verizon MA's COs. Likewise, all future physical collocation deployments must provide for such a secured arrangement. In those cases where new physical collocation arrangements cannot be provided in segregated CLEC areas with separate entrances, virtual collocation arrangements should be required.

Q. Please explain why Verizon MA believes the security risks raised by physical collocation can be best met by requiring separate rooms or segregated space – and providing a secured path or route to that space - for collocated carriers.

A. Verizon MA believes that a higher, yet reasonable, degree of security is required to ensure full network reliability, and can only be attained if collocators are located in separate and segregated areas of the CO. Providing a physical and secure barrier that prevents CLECs or others from gaining access to Verizon MA's CO equipment is necessary for several reasons.

First, while Verizon MA is permitted to escort its own vendors, the FCC and the Department require that Verizon MA provide a collocator with *unescorted* access to its equipment in the CO 24 hours a day, seven days a week. If Verizon MA is

not permitted to separate and secure that equipment, then non-Verizon employees will have unlimited access to the Company's network facilities, thereby increasing the risks of accidents and sabotage.

Second, Verizon MA requires that its own vendors adhere to the Company's "Safe Time" policy. This prohibits equipment installation or rearrangement activities within close proximity to working equipment except during late evening to early morning hours (*i.e.*, typically between 11:00 P.M. and 7:00 A.M.) when any accidental disruption to working equipment would have minimal impact on consumers. That safety policy would be undermined, and network security threatened, if separating or partitioning collocator equipment were not required, and collocator personnel could access unsecured equipment any time of the day.

Third, the number of collocators in Massachusetts COs range from one to as many as 27 CLECs per CO. Each CLEC, in turn, has many employees that would potentially have access to Verizon MA's COs. Even if Verizon employees are in the CO at the same time as the CLEC employees, they would not necessarily know which CLEC employees belonged in a particular CO and who did not (especially with the unauthorized sharing of identification badges and access cards), or on which piece of equipment a given technician was authorized to work. Physical separation of CLEC collocation equipment area and Verizon MA's equipment areas would provide Verizon MA with the ability to deter or prevent unauthorized individuals from venturing beyond their designated area into

areas where they have no reason or authority to access.[23] This provides further assurances that its network will be safer and better protected with higher and reasonably practical protection and.

Finally, placing CLEC equipment in a separate and secured area of the CO away from Verizon MA's equipment may also have the added benefit of providing not only superior, but often less expensive, security arrangements for both the Company and the collocator. This can allow easier access for the collocators' personnel and reduce the need for security cameras systems and other expensive security arrangements. Separate space that is dedicated to collocation can also be engineered with new collocation arrangements in mind, *e.g.*, to provide power and office connections likely to be requested by collocators. Provided that such space is not technically inferior to space elsewhere in the CO, Verizon MA should be permitted to require separate and secured space for all forms of physical collocation (including CCOE) to ensure the safety, security and reliability of the telecommunications network.[24]

Q. Please comment on the security concerns relating to the commingling of Verizon MA's and CLEC's equipment.

---

[23] Likewise, there are existing equipment areas in the CO where Verizon MA employees are restricted from entering, except for those employees who are properly trained to work on the equipment.

[24] It should be noted that the in its December 21, 2002, Brief on appeal, the FCC clarified its position, stating that separate rooms and entrances are permitted to address legitimate security concerns provided that the CLECs are not disadvantaged.

A. Commingling of Verizon MA's and CLEC's equipment in the same unpartitioned equipment area presents insurmountable security problems. Existing security measures, such as card readers, keys, and cameras, are simply not enough in a commingled environment absent secure partitioning, and would be cost prohibitive. Even if such security devices *could* be reasonably placed in all necessary areas in the CO, any accidental or intentional damage to Verizon MA's equipment would be exceptionally difficult to detect, much less prevent because of the close proximity of the CLEC equipment and CLEC personnel working on that equipment.

For example, video surveillance would be ineffective because when equipment is located in the same or adjacent bays, it is virtually impossible for an on-camera view to show on which piece of equipment a technician is working, let alone whether the technician has made inadvertent or intentional contact with equipment in an adjacent bay. Moreover, while video surveillance alone may provide some deterrent to interference with Verizon equipment, for the most part, it can only help determine accountability after the damage is done.

In addition, commingling raises considerable security risks because of the fundamental differences between Verizon MA's employees or vendors and CLEC employees or vendors, who would be installing and repairing equipment that is

not physically separate from the Company's equipment.[25] This is a key factor in permitting Verizon MA to require that CLEC equipment be separate and secure from the Company's equipment and not commingled. In addition, much of the equipment deployed by the CLECs looks the same as Verizon's equipment,[26] which increases the likelihood that CLEC personnel may inadvertently work on the wrong shelf - and directly or indirectly cause a service outage. Accordingly, Verizon MA should be allowed to require virtual collocation where available floor space limits preclude establishing a separate, segregated area for physical collocation.

---

[25] First, unlike Verizon's own employees, CLECs' employees are not accountable to Verizon. Verizon may escort a CLEC employee out of the CO if he/she is unauthorized or responsible for accidental or intentional damage in the CO. However, Verizon MA cannot terminate his/her employment, as it could its own employee or vendor. That distinction creates an incentive for Verizon MA's workforce and vendors to follow proper procedures and exercise care and caution when working around Verizon MA's equipment, and conversely a disincentive for CLEC employees or agents. In fact, the CLEC employee or agent can re-enter Verizon MA's CO at another time using someone else's access card, or may accompany a co-worker with a valid access card.

Second, Verizon MA has no way of knowing whether the CLEC employee has been adequately trained to work on equipment in a CO environment. Verizon's own employees undergo significant training before they are permitted to work in the CO, and some are even specifically trained and authorized to work on particular CO equipment, as noted above. Untrained CLEC employee/agent may accidentally damage Verizon MA's equipment while working on the CLEC's equipment, or may inadvertently work on Verizon MA's equipment in a commingled environment.

Finally, both because Verizon MA can carefully screen its employees and because Verizon MA is better able to hold its own employees and vendors accountable, physical segregation of CLEC equipment is preferred. This will minimize the likelihood that third parties, who have no legitimate business in Verizon's COs, will gain access to them.

[26] To the extent that CLEC and Verizon equipment may be the same, this also increases the likelihood that "spare parts" on hand in Verizon's CO will be "poached" if needed by a collocated carrier for provisioning or maintenance purposes, based on Verizon's actual experience nationwide in physically collocated COs. This too can result in service outages, as Verizon has experienced firsthand when CLECs have borrowed "in-use" Verizon equipment parts for their own needs, without Verizon's permission or prior knowledge

Q. What protections do CLECs have in a physical collocation environment?

A. CLECs already have adequate safeguards available to them to protect their equipment. Verizon MA provides "caged" physical collocation and SCOPE arrangement in separate collocation areas that are normally secured, with entry limited to collocators by means of magnetic coded cards, keys or keyed cipher locks. In addition, "caged" collocation provides for a wire mesh enclosure that surrounds the area allocated to the individual CLEC. That cage is provisioned with a locking door to which the CLEC has the key.

CLECs opting for additional security can request installation of tops on their physical cages, or may elect to install locking cabinets or covers for their equipment in caged or cageless collocation arrangements. Similar security arrangements for Verizon MA's equipment would not be possible if separate space was not required and commingling of equipment was permitted.

Q. Please explain the security concerns raised by cageless collocation, and Verizon MA's proposed security measures to address those concerns.

A. Cageless collocation or CCOE differs from "caged" physical collocation and SCOPE in that it does not require the establishment of separate space for the collocated carrier. Indeed, CCOE is used where *separate* physical collocation space is not available due to space restrictions in a particular CO. In fact, some existing CCOE arrangements in Massachusetts are *unsecured*, which means that

they are located in areas where Verizon MA's equipment is already placed and cannot be segregated. This configuration presents serious security concerns.

It is virtually impossible to provide adequate security for Verizon MA's facilities in an unsecured environment where CLEC personnel is allowed 24 hour a day, seven days a week unescorted access. Such conditions lead to increased potential opportunities for accidental or intentional dislodging of Verizon MA's connections or damage to other Company equipment that is exposed and physically unseparated from collocators' equipment. Verizon MA must be able to protect its own equipment without having to resort to massive reconstruction and reengineering. Placing locked cabinets around Verizon MA's equipment is not technically or operationally feasible without moving equipment to make space for such cabinets and without reconstructing the entire heating, ventilation, and air conditioning system in its COs. In addition, even if this were technically feasible, it would not be practicable because of the amount of available space in most Verizon MA COs.

Verizon MA estimates that approximately 13 of the 27 CCOE arrangements in Massachusetts are placed in unsecured areas within nine COs. Because unsecured CCOE arrangements pose unacceptable and unnecessary risks to the security and reliability of Verizon MA's network, the Company recommends that, in those limited instances, the existing arrangements must either be rearranged to a

segregated collocated area within the CO or converted to virtual collocation, in place if feasible.

Likewise, to ensure that network safety and reliability is maintained, Verizon MA proposes that future CCOE arrangements only be placed in separate and secured collocation areas. This approach is not only warranted for security reasons, but is consistent with the *FCC Remand Order*, which expanded Verizon MA's rights to separate and segregate physically collocated equipment within its premises.

Q. How does Verizon MA propose to address security issues raised by collocated carriers' need for reasonable access to shared facilitiesin the CO?

A. The FCC has found that collocated carriers are entitled to reasonable access to shared facilities (*e.g.*, temporary staging areas, loading docks, restrooms, and elevators) in Verizon MA's COs. *FCC Advanced Services Order* at ¶ 49. In some COs, this means that CLECs must traverse areas where Verizon MA's equipment is located to access these shared facilities. Thus, while physical collocation arrangements may be separate and secure, access to shared facilitiesis not. For security reasons, access to shared facilities also needs to be limited to where these facilities can only be accessed *without* entry to Verizon MA's equipment areas.

Verizon MA has not quantified how many COs with physical collocation do <u>not</u> have a physically secured passage or access to shared facilitiesseparated from

Verizon's equipment space.[27] However, Verizon MA proposes to determine where partitioning is feasible to protect Verizon MA's network from inadvertent or deliberate harm while providing collocators with "reasonable access" to common areas. In those COs where such partitioning is not feasible, CLEC access to other areas outside of the existing physical collocation arrangements is not required, and should not be permitted. Verizon MA will, however, continue to coordinate, at the carrier's expense, pre-arranged access to certain common areas, such as temporary staging areas and loading docks, for the delivery and unpacking of collocated carriers' equipment for a given CO. This is the only reasonable and effective means of providing adequate network security in a collocated environment where separate space or physical barriers cannot be erected to segregate, secure and protect Verizon MA's equipment.

Q. Please describe the security concerns raised by CRTEE arrangements, and Verizon MA's proposed security measures to address those concerns.

A. Verizon MA offers CRTEE in accordance with the FCC's collocation requirements. The FCC is currently reviewing the appropriate security measures for such arrangements in connection with its *Remand Order*. *FCC Reconsideration Order* at ¶ 104. Although no CRTEE arrangements currently exist in Massachusetts, Verizon MA believes that the Department should address

[27] In most smaller COs, this basically means that collocators have unfettered access to roam about the CO.

the unique security problems raised by RTs in this proceeding in the event that CRTEE is requested by a CLEC in the future.

As explained in Attachment 3, RTs are freestanding structures (e.g., CEVs, huts or cabinets) located outside of the CO that house telecommunications electronic equipment. Because RTs house much of the same costly and delicate equipment housed in a CO, they present the same opportunities for service disruption, equipment tampering and theft, as discussed above. However, securing RTs is even more problematic because of their extremely small size and their location.

There are more than 2000 RT structures in Massachusetts. Inadvertent or improper actions within the tightly engineered and confined space of RT can cause service disruptions for many customers. Customers served through RTs would be as isolated from critical emergency services and other communications just as if the damage originated in the CO. However, because redundant network facilities in an RT are more closely located with other facilities, the likelihood of service-affecting consequences is even greater than in the CO.

Unlike a CO, in most cases, it would be practically impossible to segregate Verizon MA's equipment into separate space in an RT. As explained in Attachment 3, none of the RT structures is designed to enable Verizon MA to secure its equipment, as well as power, from access by other carriers. For example, CEVs and huts are sized so that a technician can enter the enclosure and gain access to the equipment and wiring in the limited space available. RT

structures typically have no space for more than one or two individuals, at most, at one time. Partitioning or securing equipment inside a locked enclosure inside the small RT is, therefore, not a practical solution because of the additional space such an enclosure would occupy and the lack of excess space in the confined RT structure.

Likewise, providing secure access to RT locations would become an increasingly difficult problem to administer and control. Access to the various types of RTs include padlocks, keys and special tools. Retrofitting RTs for other security mechanisms (*e.g.*, placing card readers or cameras) to give other carriers access would be a significant and costly undertaking. This also assumes that those methods alone would provide adequate network security – which they would not, for the reasons discussed above. The only way to ensure adequate security at an RT is to allow Verizon MA to limit RTs to virtual collocation or, in the alternative, to require a security escort for the CLEC technicians.

Virtual collocation will enable Verizon MA to reasonably protect its equipment because only Company technicians would be allowed to install and maintain equipment that the collocated carriers supply. This would make more efficient use of the limited available space because it eliminates the need to segregate equipment within the RT. It would also prevent one carrier's collocated equipment from being inadvertently affected by another carrier's technician working in the limited space. In addition, Verizon technicians are properly

trained on taking necessary precautions in entering CEVs, which must be properly ventilated and checked for foreign, gaseous odors prior to entering the structure.

If, however, the Department does require physical collocation at RTs, which it should not, then the only practical means of protecting Verizon MA's network facilities is to require the use of escorts to accompany collocators that *maintain* their own equipment. Because of the greater possibility of accidental or intentional damage, collocators should not, however, be permitted to install their own equipment in RTs, even under a physical collocation arrangement.

Q. How does allowing CLEC access to manholes present increased security concerns?

A. As part of the FCC's collocation requirements, CLECs may have access to Verizon MA's manholes in deploying their own fiber optic entrance cable.[28] Verizon MA's manholes are used access to underground inter-office and feeder/distribution facilities, and are often small, dark and densely filled. Because the cramped working area increases the potential for damaging other proximate network facilities, Verizon MA requires the presence of a Contract Work Inspector ("CWI") when CLECs require access to manholes to place facilities. Applicable terms and conditions are contained in Verizon's standard conduit

[28] *Local Competition Order*, at ¶ 1119; *see also* 47 U.S.C. § 251(b)(4) (citing LEC's "duty to afford access to the poles, ducts, conduits, and rights-of-way of such carrier to competing providers of telecommunications services on rates, terms, and conditions that are consistent with section 224" of the Telecommunications Act of 1996).

occupancy agreement, which must be executed by a CLEC prior to placing its facilities in Verizon MA's conduit systems. Although Verizon MA has experienced some CLEC violations of these security practices, the Company proposes no change in its current practices at this time.

Q. Please comment on Verizon MA's proposal to classify certain select COs as "critical" sites that would provide virtual collocation only, even if physical collocation space were otherwise available.

A. Verizon MA proposes to work with the Department to identify those "critical" COs where virtual collocation only should be required. The key factors to consider in determining the critical nature of a central office may include: (1) the type of switch or signaling elements housed in a CO; (2) the presence of critical customers (*e.g.*, major airport, military installation, government agencies, and/or nuclear power plant) served by a CO; and (3) the number of access lines and special services circuits served by a CO. For example, a CO may be more critical if it houses a tandem switch, an E911 tandem switch, and/or STP equipment that are the "lifeline" to numerous subtending switches throughout Massachusetts.

Accidental or intentional damage to the network resulting in disruption of existing service in those particular COs could pose national security risks, endanger the health, safety and welfare of many more lives, and jeopardize the operations of major businesses, public safety, and government agencies, as well as advanced technology companies and other institutions that are involved in national security

matters. Therefore, the security and network reliability of Verizon's infrastructure in serving those select COs would be of national importance.

Based on this preliminary criteria, there is a handful of Massachusetts COs that would meet this criteria and be designated as "critical," providing *only* for virtual collocation arrangements for security reasons. Verizon MA would recommend that any existing physical collocation arrangements in those critical COs be converted to virtual collocation arrangements. Where feasible, physical collocation would be converted to virtual "in place," thereby minimizing any added security costs borne by the CLECs.

COST RECOVERY PRINCIPLES

Q. Who should bear the costs associated with enhanced security measures in Verizon MA's physically collocated COs or RTs?

A. While Verizon MA has not determined the costs associated with its proposed collocation security plan,[29] the Company believes that it should be permitted to recover those costs from the cost-causer, *i.e.*, the collocated carriers. To the extent that conversions of existing physical collocation arrangements to virtual collocation are required under the terms and conditions as described above,

[29] "Reasonable security costs" related to collocation and recoverable from the CLECs may include the costs of standard security devices, such as electronic card readers, security cameras, etc., as well as the costs associated with the construction of new walls, structures, or entrances for separate space and/or the use of escorts.

Verizon MA will endeavor to transfer those arrangements "in-place," thereby minimizing the costs passed on to the CLECs.

Allowing Verizon MA to recover its additional security-related costs from the collocated carriers is fully consistent with the longstanding economic cost recovery principle of cost causation. As previously explained, COs and RTs were originally designed to protect the equipment from within, meaning that the facilities were locked and only authorized Company employees were permitted access to those sites. However, with physical collocation, multiple carriers' equipment is now placed in Verizon MA's CO, and many more individuals are allowed access to Verizon MA's facilities.

For example, in Massachusetts alone, there are 46 CLECs who have currently have 948 physical collocation arrangements and 4 virtual collocation arrangements in 169 Verizon MA COs. This influx of "foot traffic" in the CO dramatically increases the security risks to the network infrastructure and directly affects the type of security measures that can and must be imposed. Those same security methods would not otherwise be required if Verizon MA were the only carrier occupying the CO space. Accordingly, because the collocated carriers benefit from access to Verizon MA's COs and RTs, and reasonably cause the added security costs to be incurred, they – not Verizon MA – should bear the full costs associated with the additional security measures taken to protect the network from harm.

Q. Does this conclude Verizon MA's testimony?

A. Yes.